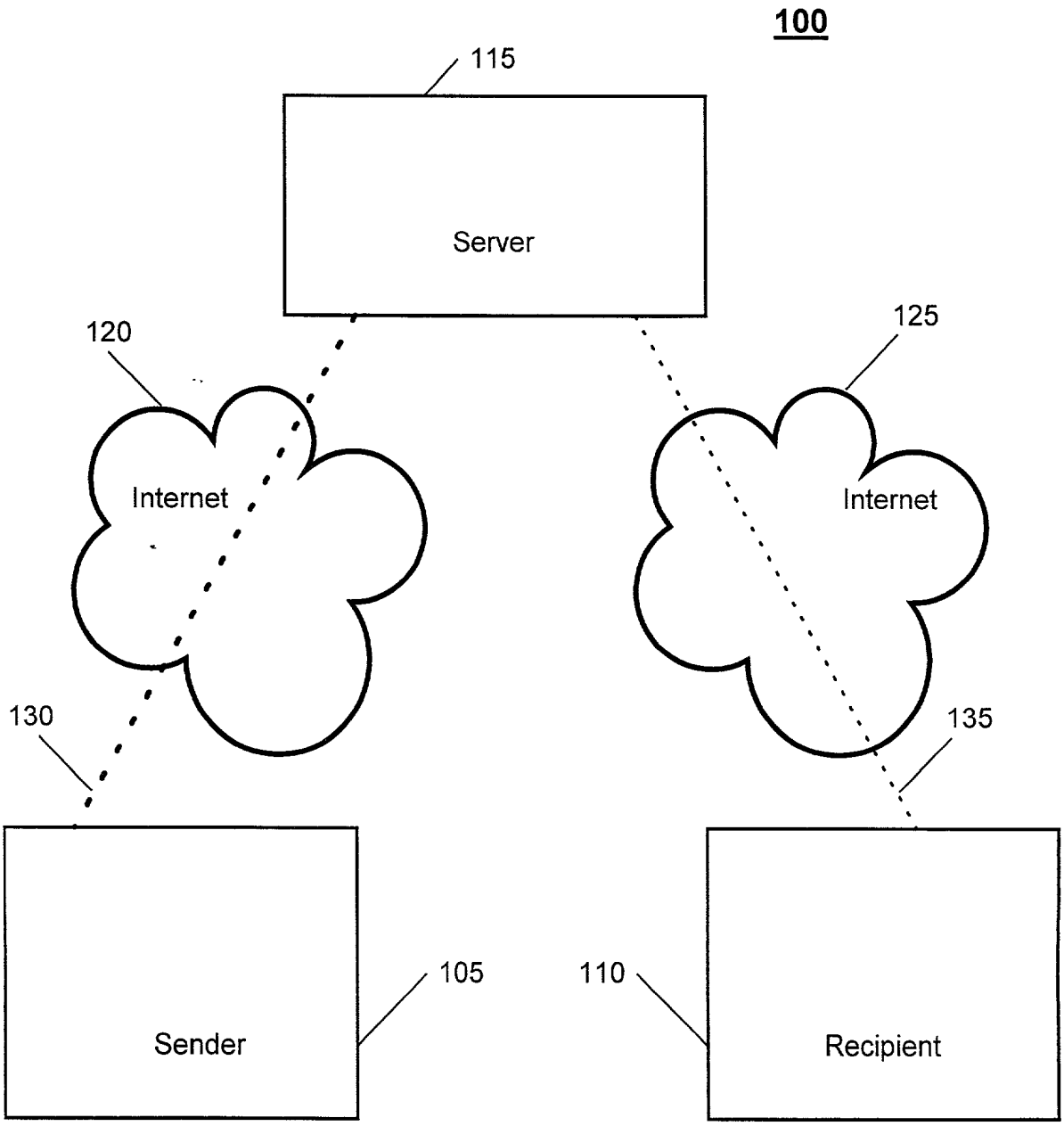

100
115
Server
120
125
Internet
Internet
130
135
105
110
Sender
Recipient

Figure 1

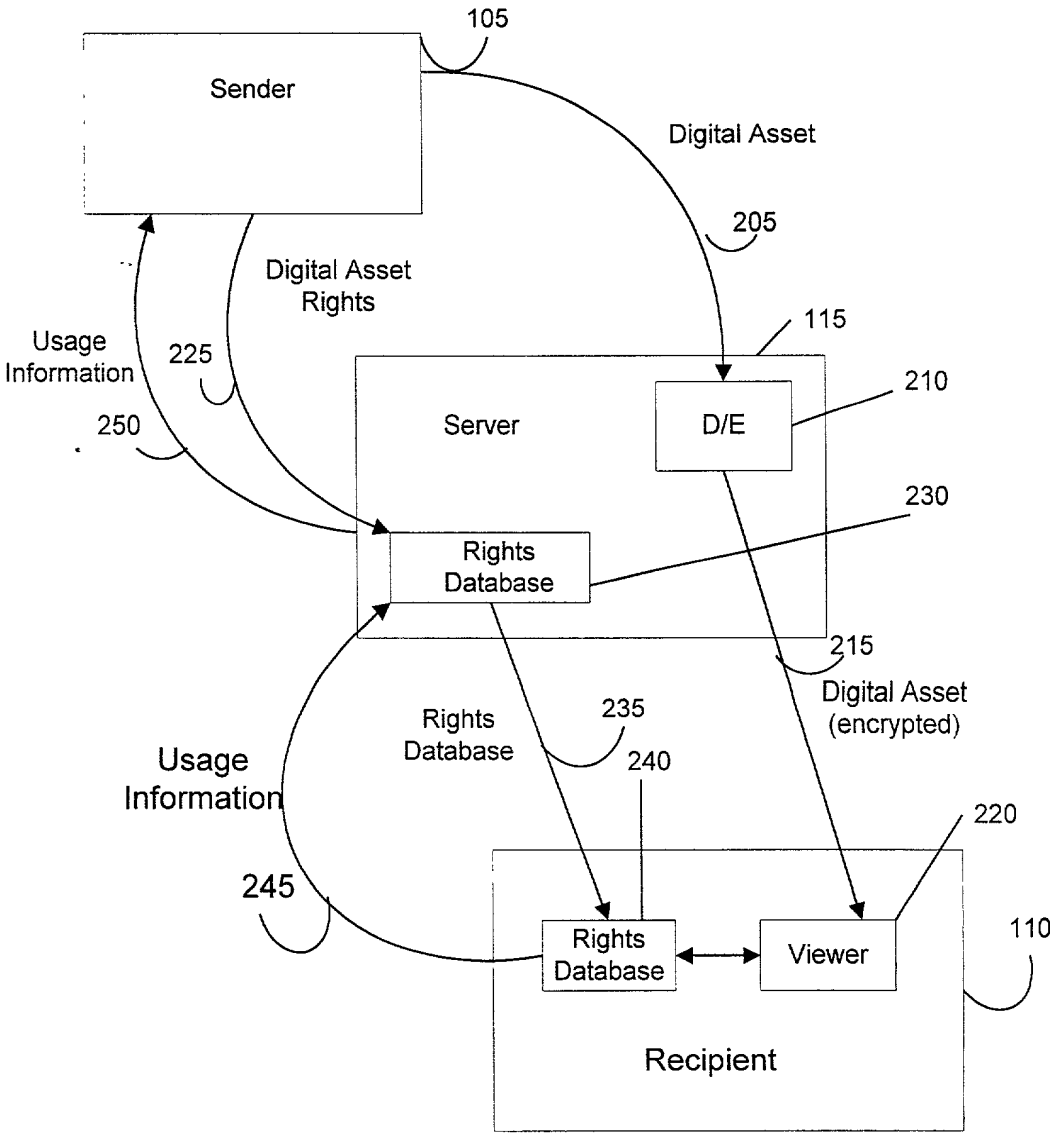

105
Sender
Digital Asset
205
Digital Asset
Rights
115
Usage
Information
225
Server
D/E
210
250
230
Rights
Database
215
Digital Asset
(encrypted)
Rights
Database
235
240
Usage
Information
220
245
Rights
Database
Viewer
110
Recipient

Figure 2

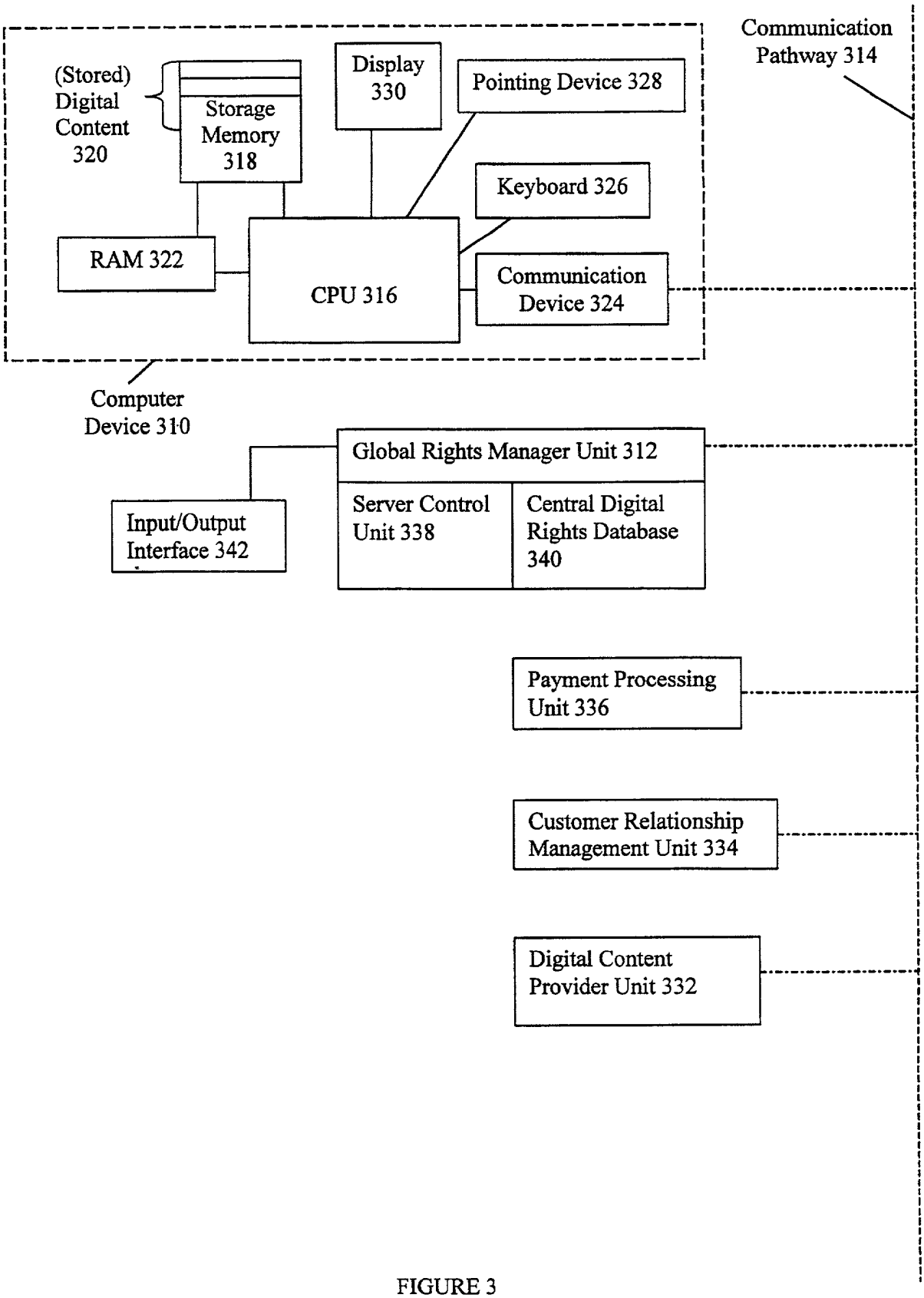

Communication Pathway 314
(Stored) Digital Content 320
Storage Memory 318
Display 330
Pointing Device 328
Keyboard 326
RAM 322
CPU 316
Communication Device 324
Computer Device 310
Global Rights Manager Unit 312
Server Control Unit 338
Central Digital Rights Database 340
Input/Output Interface 342
Payment Processing Unit 336
Customer Relationship Management Unit 334
Digital Content Provider Unit 332

FIGURE 3

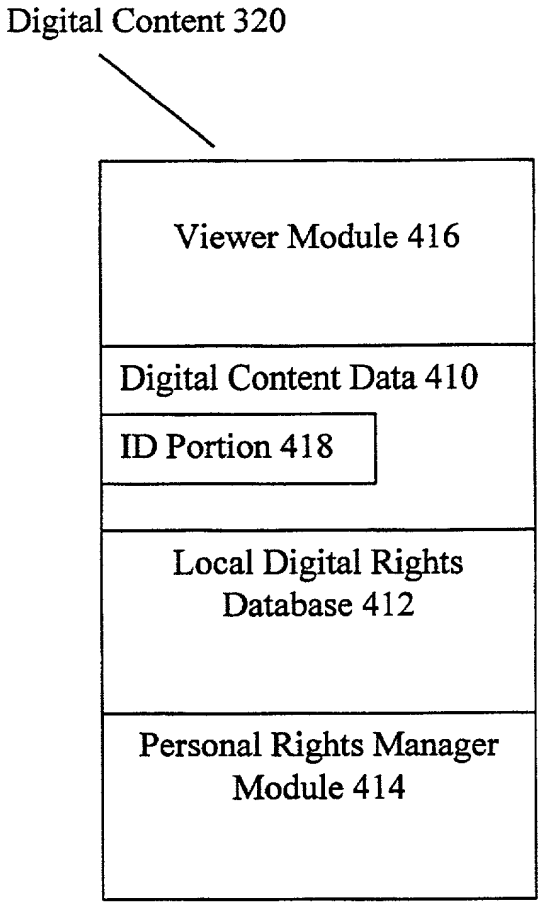

Digital Content 320
Viewer Module 416
Digital Content Data 410
ID Portion 418
Local Digital Rights Database 412
Personal Rights Manager Module 414

Figure 4

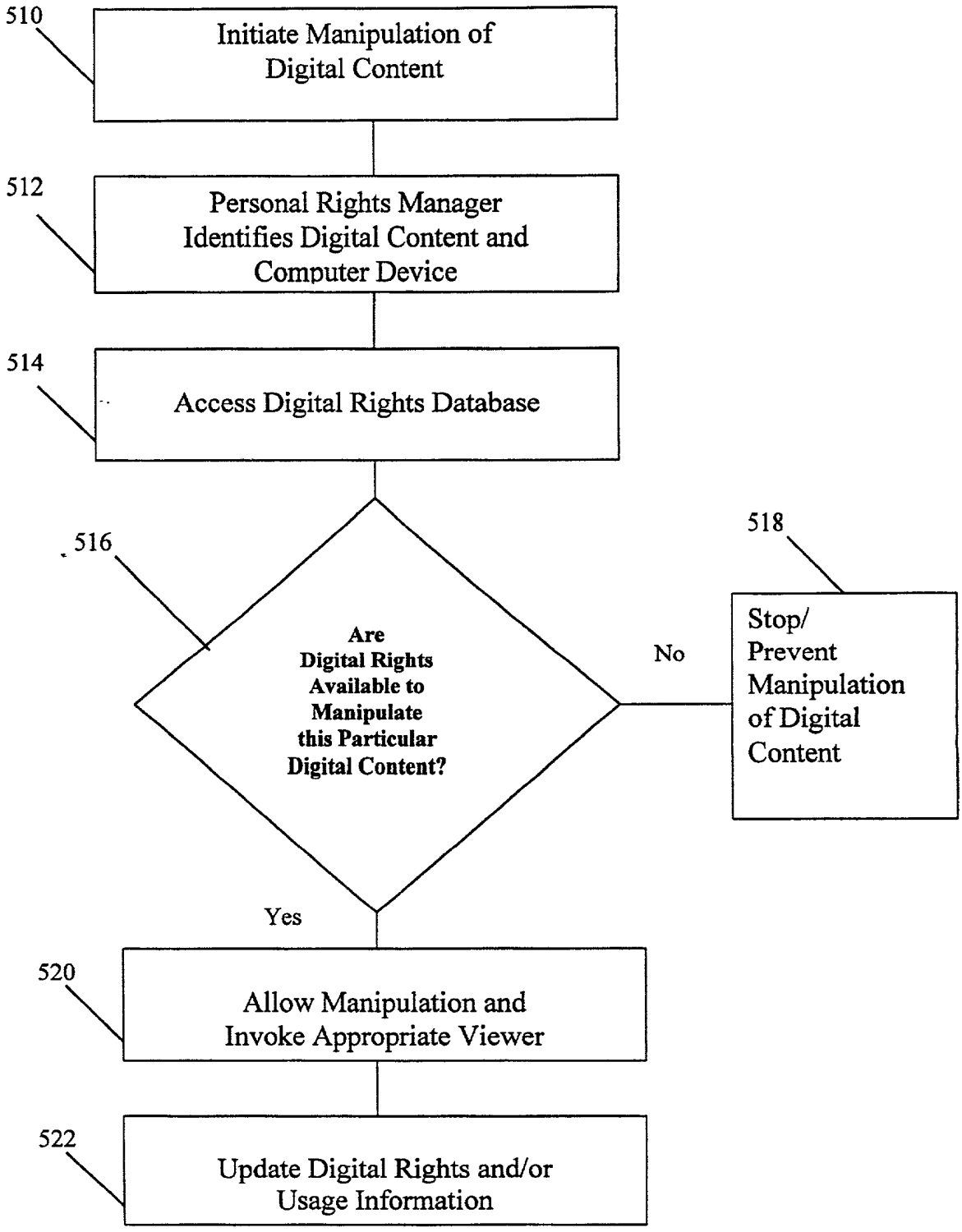

510
Initiate Manipulation of Digital Content
512
Personal Rights Manager Identifies Digital Content and Computer Device
514
Access Digital Rights Database
516
Are Digital Rights Available to Manipulate this Particular Digital Content?
No
518
Stop/ Prevent Manipulation of Digital Content
Yes
520
Allow Manipulation and Invoke Appropriate Viewer
522
Update Digital Rights and/or Usage Information

Figure 5

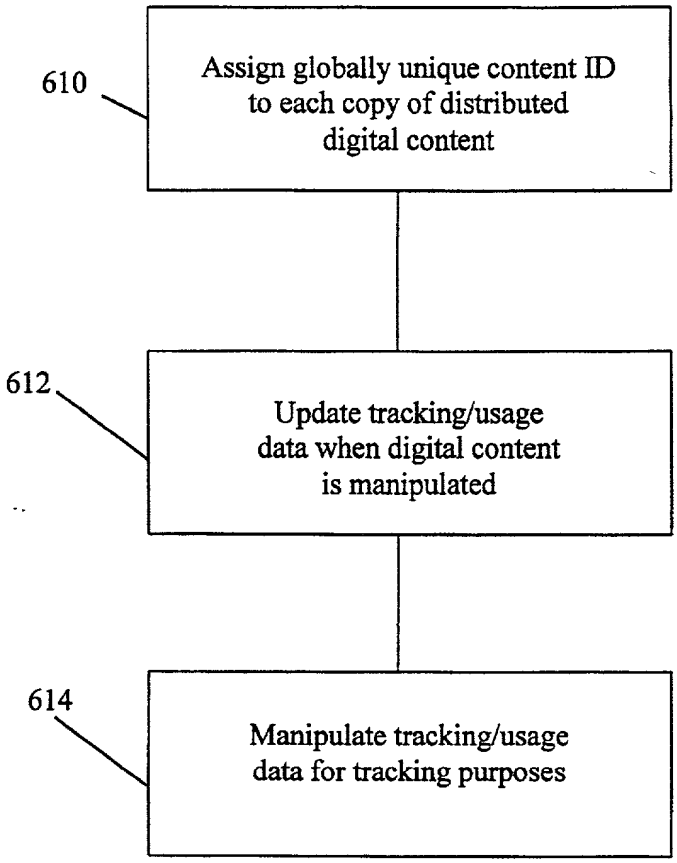

610
Assign globally unique content ID to each copy of distributed digital content
612
Update tracking/usage data when digital content is manipulated
614
Manipulate tracking/usage data for tracking purposes

Figure 6

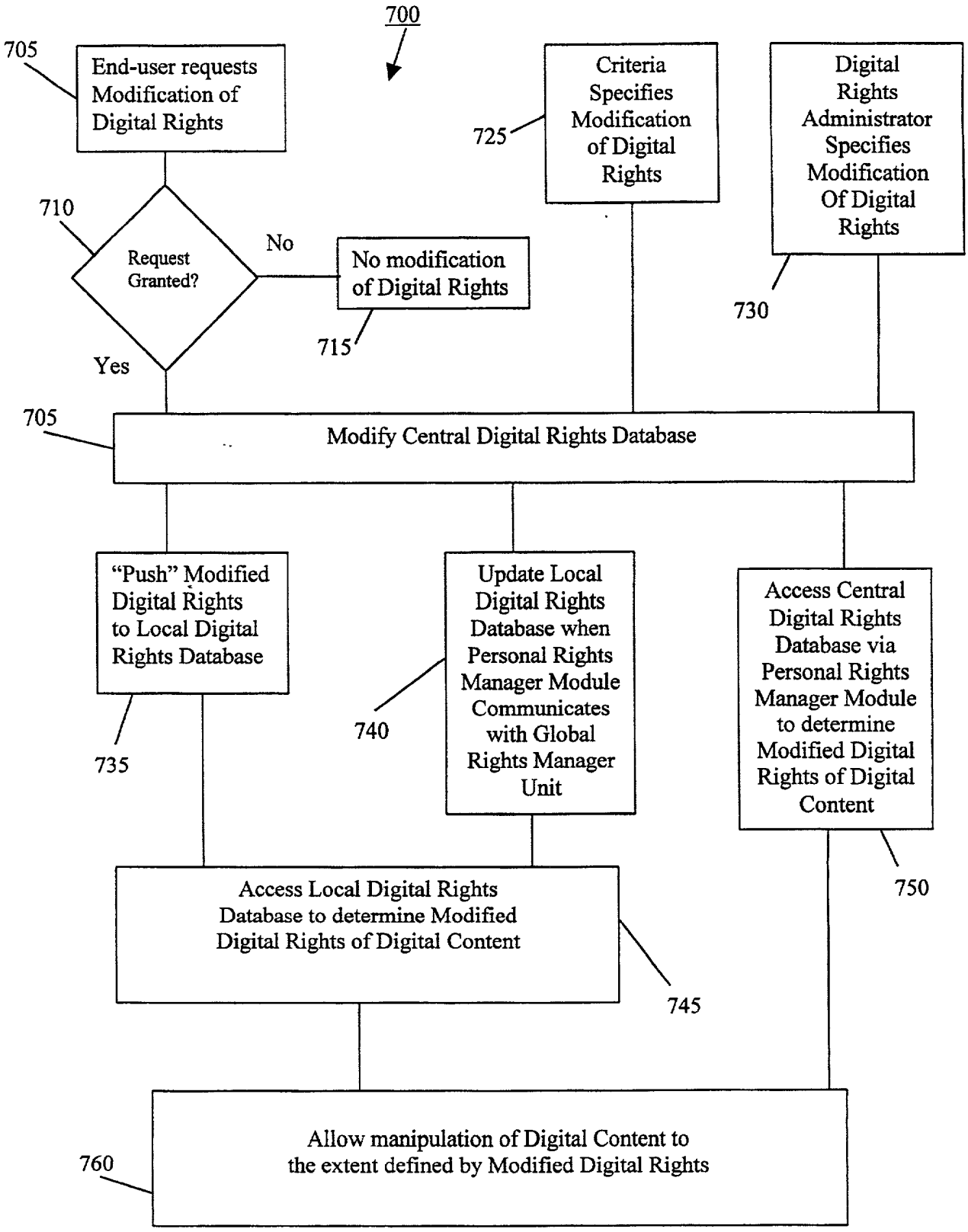

700
705
End-user requests Modification of Digital Rights
710
Request Granted?
No
No modification of Digital Rights
715
Yes
725
Criteria Specifies Modification of Digital Rights
730
Digital Rights Administrator Specifies Modification Of Digital Rights
705
Modify Central Digital Rights Database
"Push" Modified Digital Rights to Local Digital Rights Database
735
740
Update Local Digital Rights Database when Personal Rights Manager Module Communicates with Global Rights Manager Unit
Access Central Digital Rights Database via Personal Rights Manager Module to determine Modified Digital Rights of Digital Content
750
Access Local Digital Rights Database to determine Modified Digital Rights of Digital Content
745
760
Allow manipulation of Digital Content to the extent defined by Modified Digital Rights

Figure 7

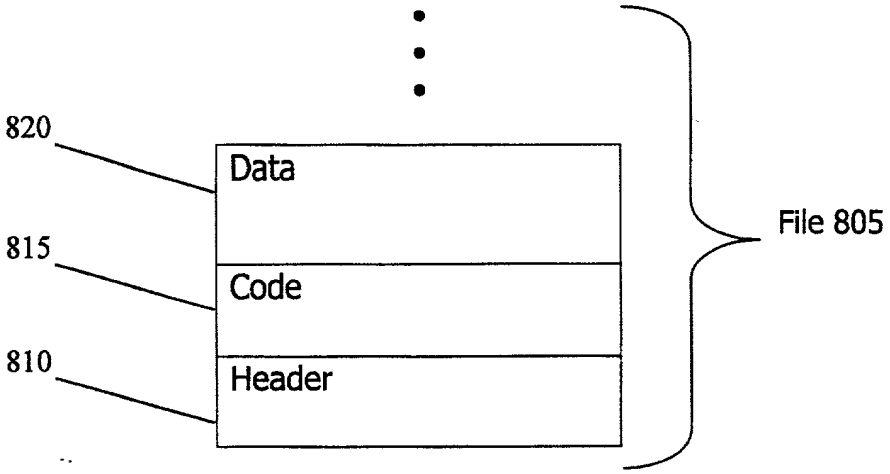


FIGURE 8A

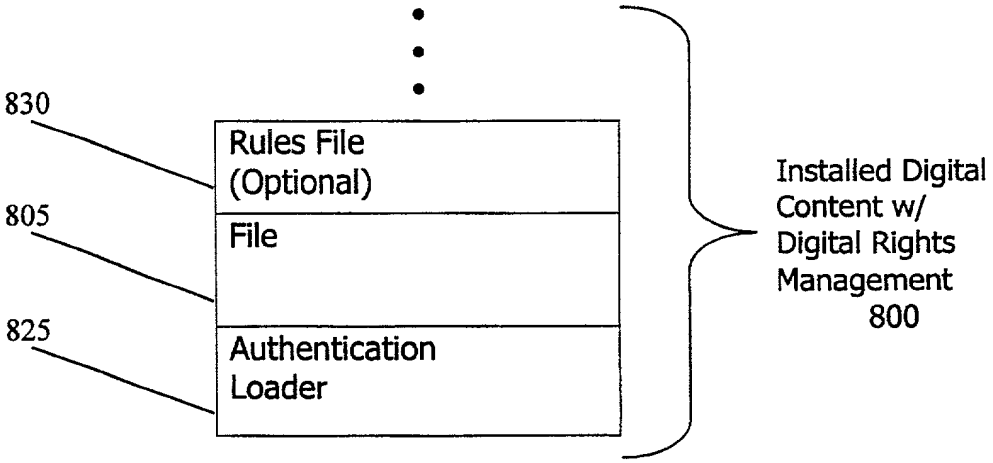


FIGURE 8B

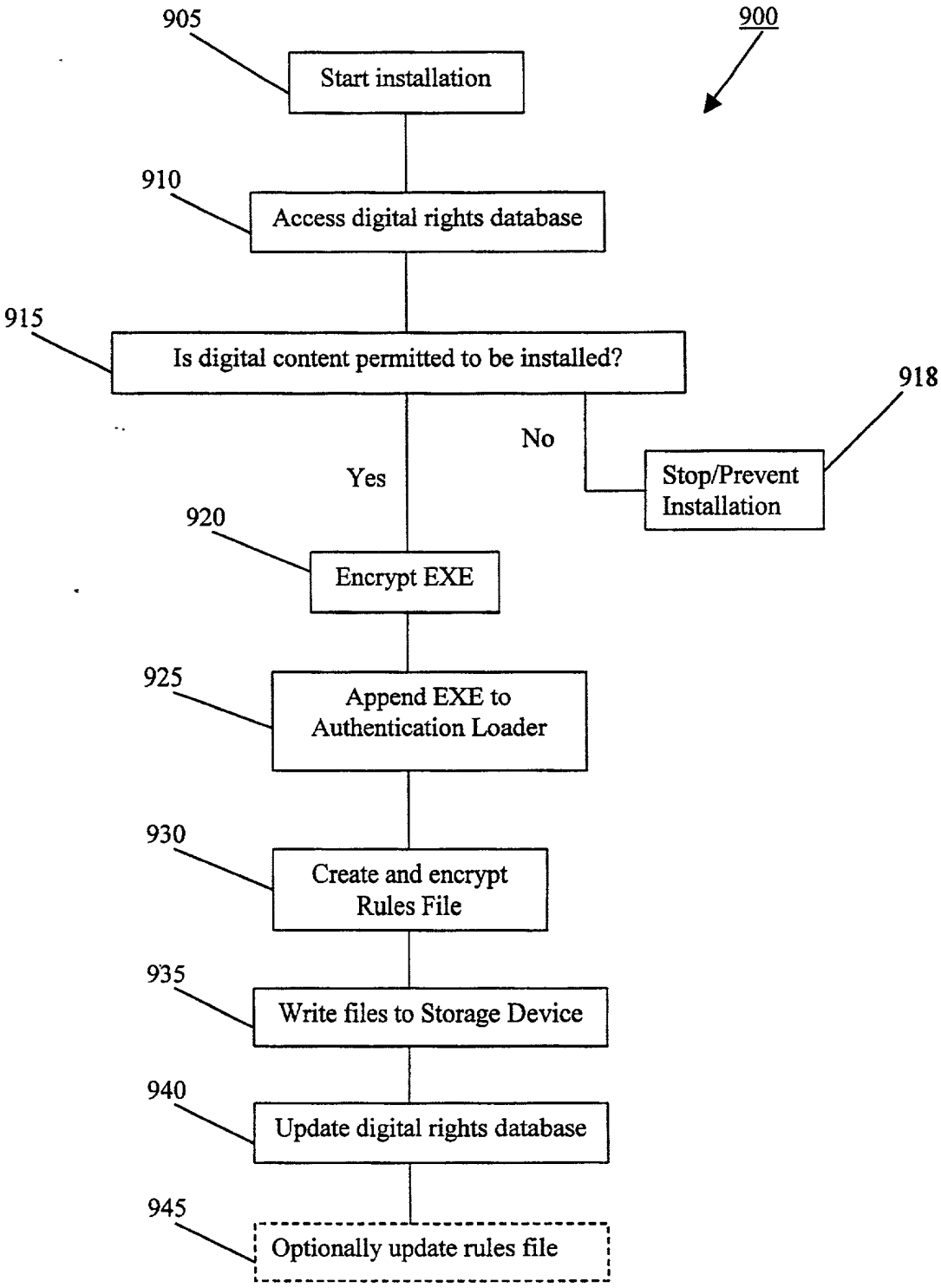

905
Start installation
900
910
Access digital rights database
915
Is digital content permitted to be installed?
No
918
Stop/Prevent Installation
Yes
920
Encrypt EXE
925
Append EXE to Authentication Loader
930
Create and encrypt Rules File
935
Write files to Storage Device
940
Update digital rights database
945
Optionally update rules file

FIGURE 9

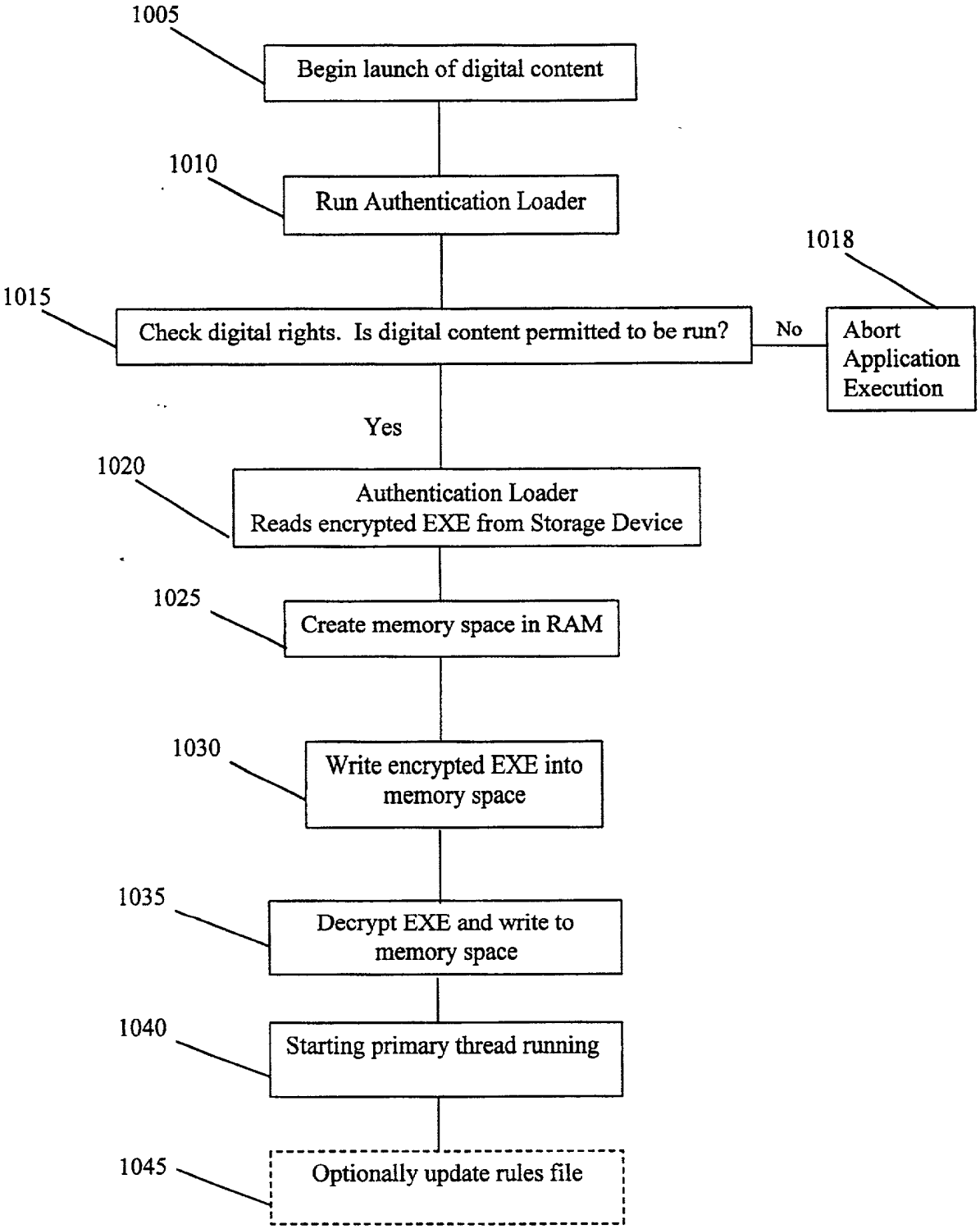

1005
Begin launch of digital content
1010
Run Authentication Loader
1018
1015
Check digital rights. Is digital content permitted to be run?
No
Abort Application Execution
Yes
1020
Authentication Loader Reads encrypted EXE from Storage Device
1025
Create memory space in RAM
1030
Write encrypted EXE into memory space
1035
Decrypt EXE and write to memory space
1040
Starting primary thread running
1045
Optionally update rules file

FIGURE 10

Fig. 11

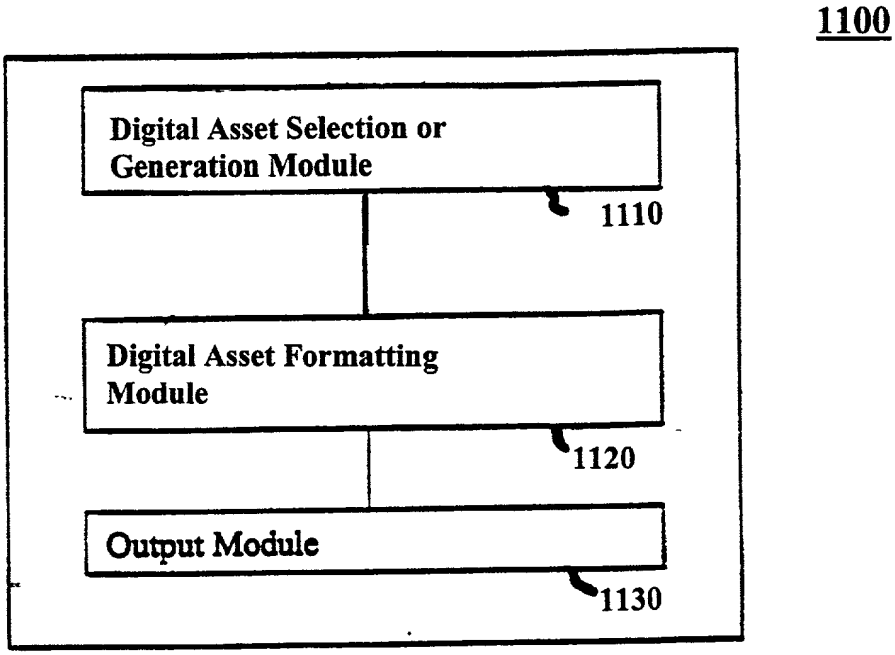

1100
Digital Asset Selection or Generation Module
1110
Digital Asset Formatting Module
1120
Output Module
1130

Fig. 12

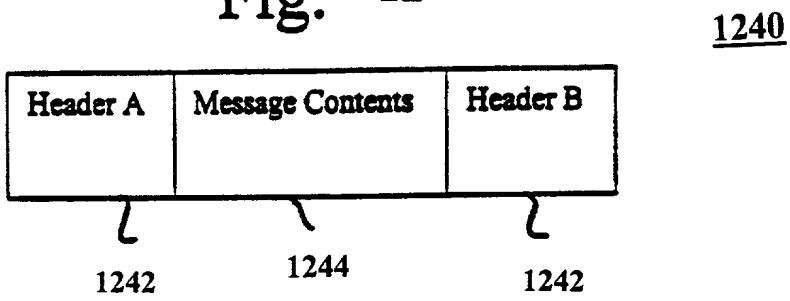
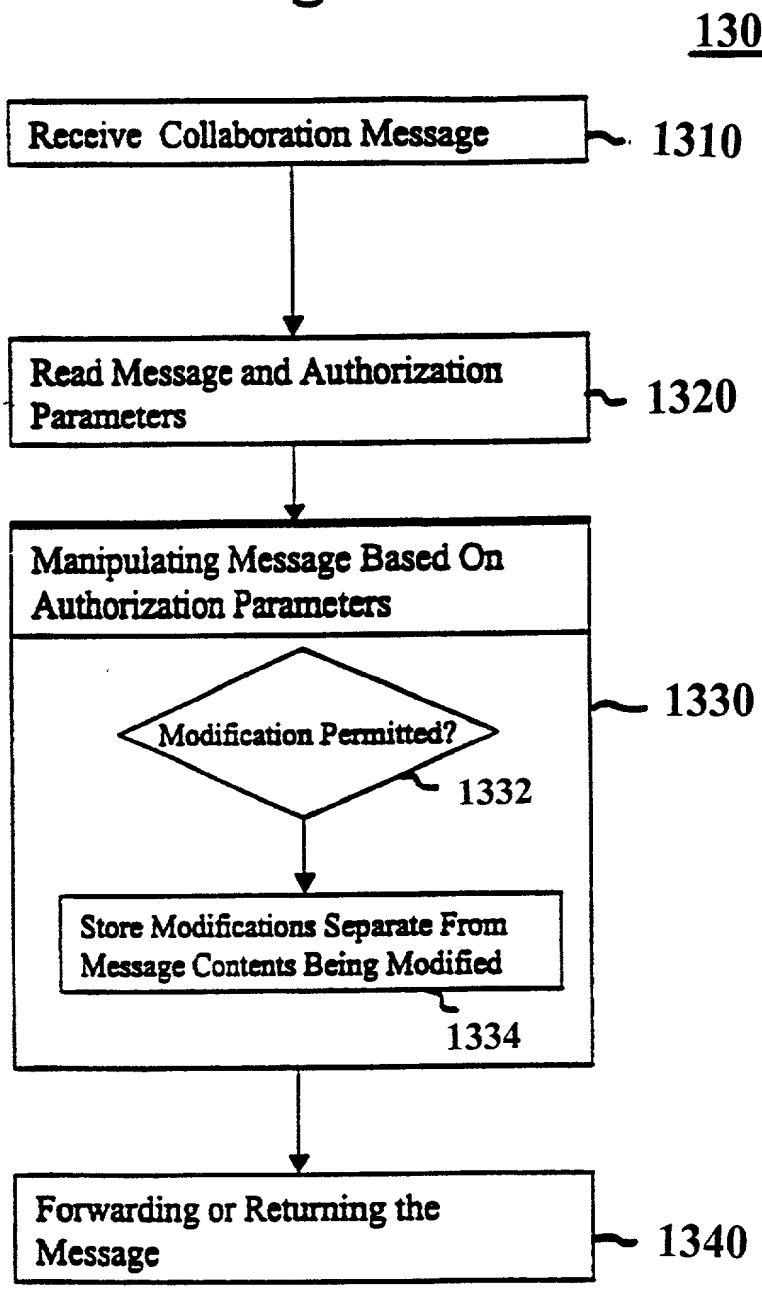

1240
Header A
Message Contents
Header B
1242
1244
1242

Fig. 13


1300
Receive Collaboration Message
1310
Read Message and Authorization Parameters
1320
Manipulating Message Based On Authorization Parameters
Modification Permitted?
1332
Store Modifications Separate From Message Contents Being Modified
1334
1330
Forwarding or Returning the Message
1340

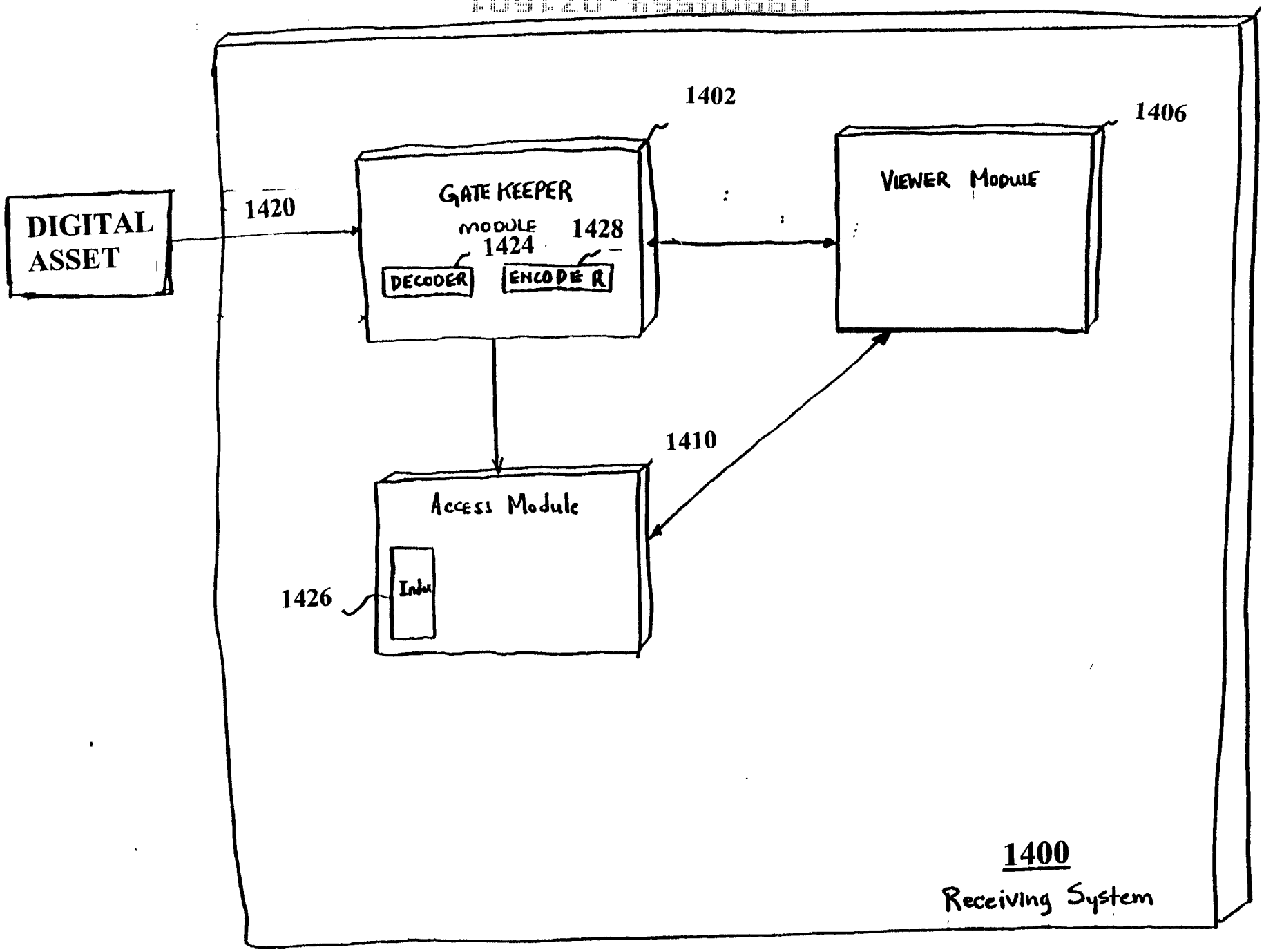

1402
1406
DIGITAL ASSET
1420
GATE KEEPER
MODULE
1428
1424
DECODER
ENCODER
VIEWER MODULE
1410
Access Module
1426
Index
1400
Receiving System

FIG. 14

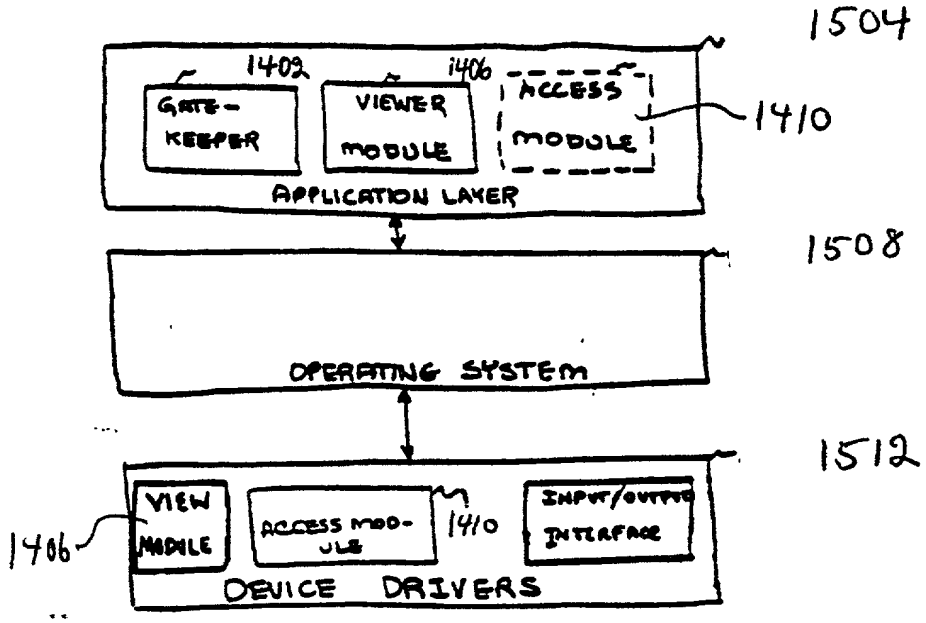

1504
1402
1406
GATE-KEEPER
VIEWER MODULE
ACCESS MODULE
1410
APPLICATION LAYER
1508
OPERATING SYSTEM
1512
VIEW MODULE
1406
ACCESS MODULE
1410
INPUT/OUTPUT INTERFACE
DEVICE DRIVERS

FIG. 15

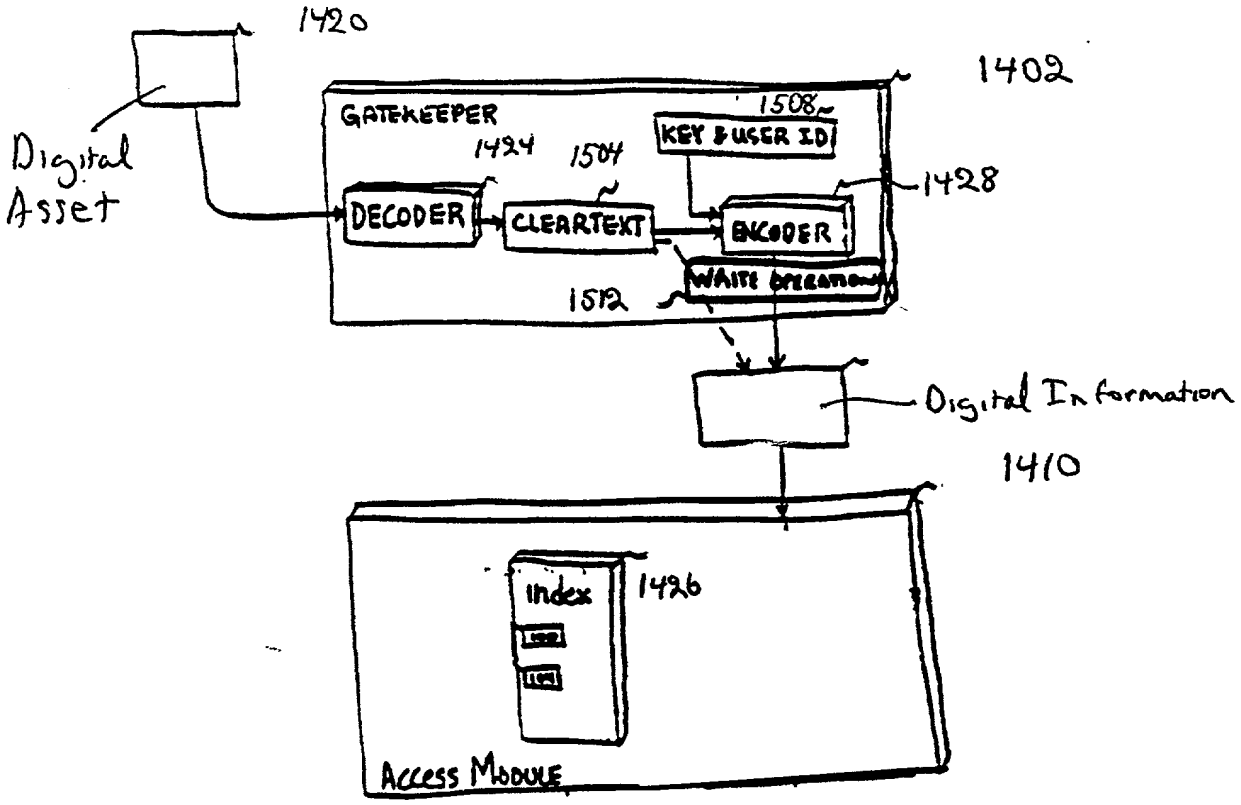

1420
Digital Asset
1402
GATEKEEPER
1508
KEY & USER ID
1424
1504
DECODER
CLEARTEXT
ENCODER
1428
WHITE BREAKER
1512
Digital Information
1410
Index
1426
Access Module

FIG. 16

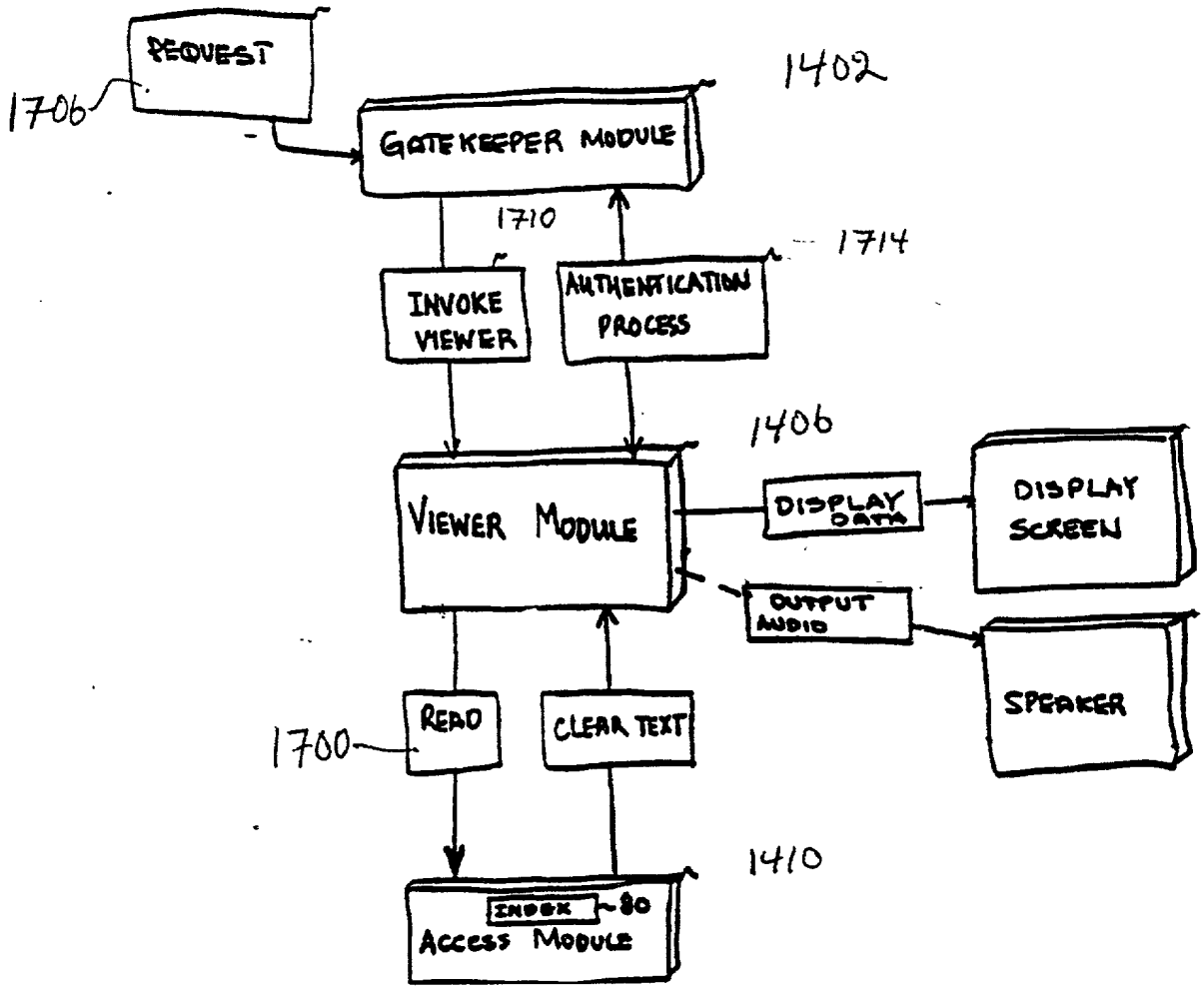

REQUEST
1706
1402
GATEKEEPER MODULE
1710
1714
INVOKE VIEWER
AUTHENTICATION PROCESS
1406
VIEWER MODULE
DISPLAY DATA
DISPLAY SCREEN
OUTPUT AUDIO
SPEAKER
1700
READ
CLEAR TEXT
1410
INDEX
80
ACCESS MODULE

FIG. 17

TOSTZO"A9Sh0660

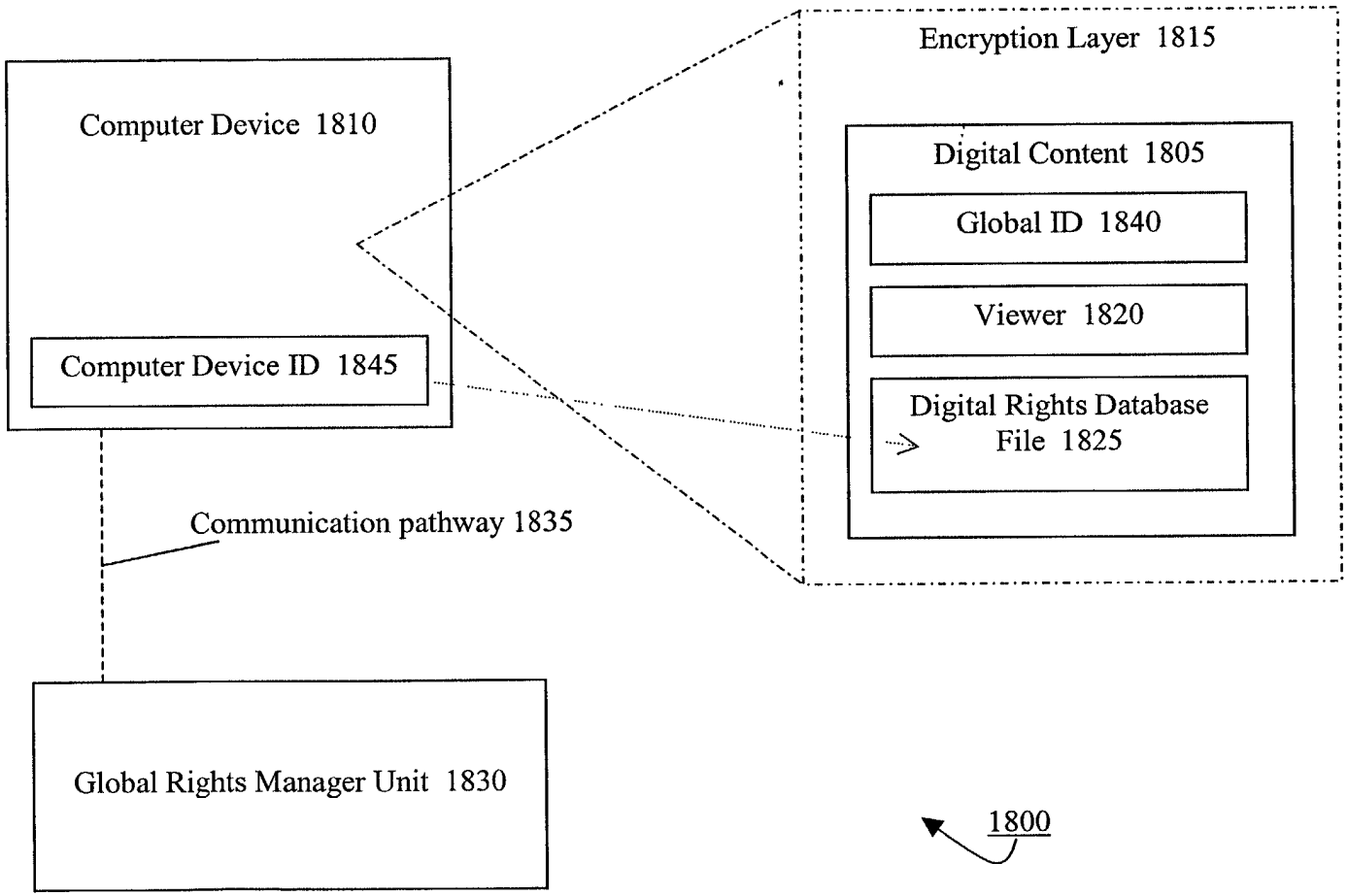


FIGURE 18

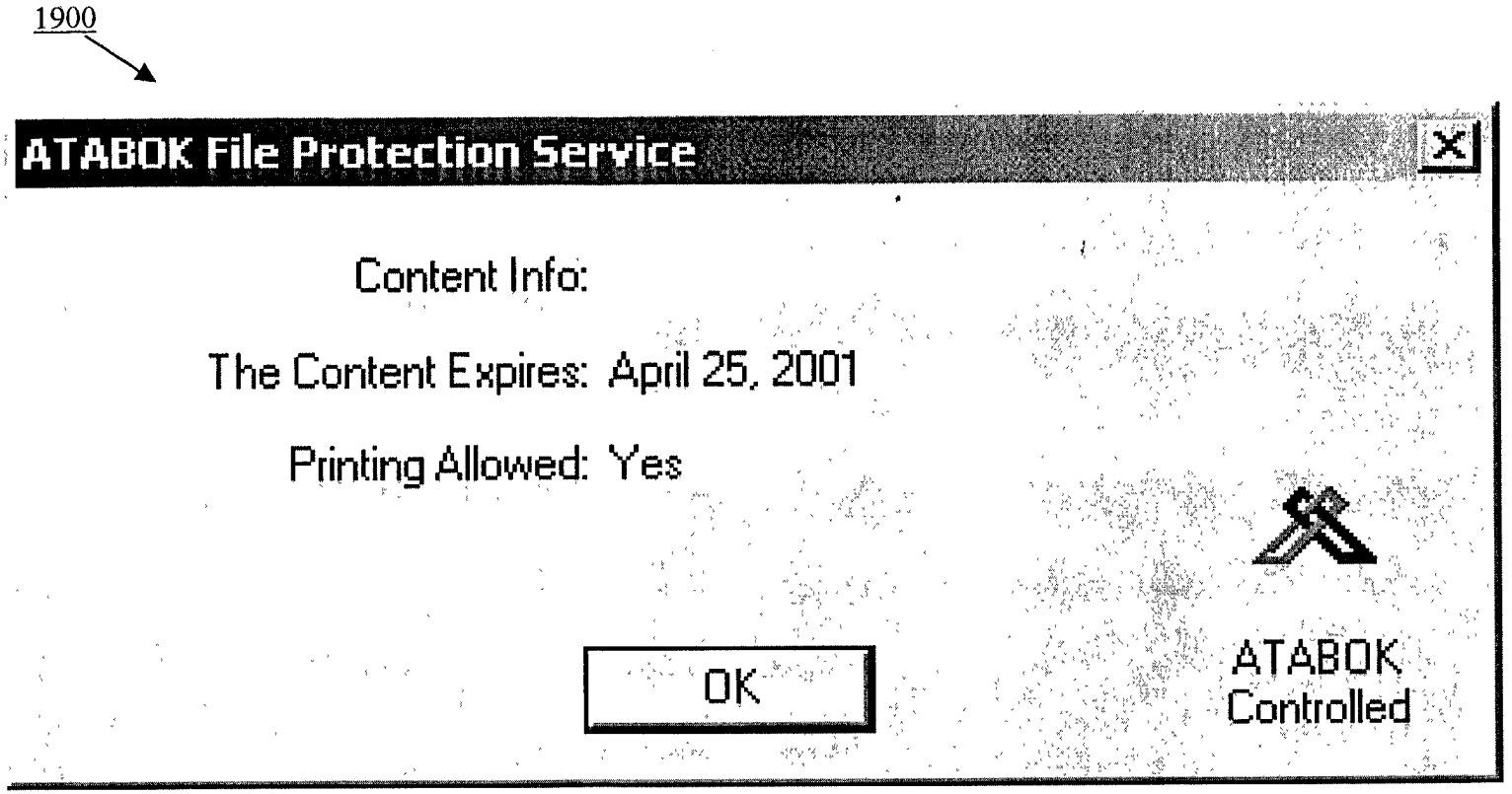

1900
ATABOK File Protection Service
Content Info:
The Content Expires: April 25, 2001
Printing Allowed: Yes
OK
ATABOK
Controlled

FIGURE 19

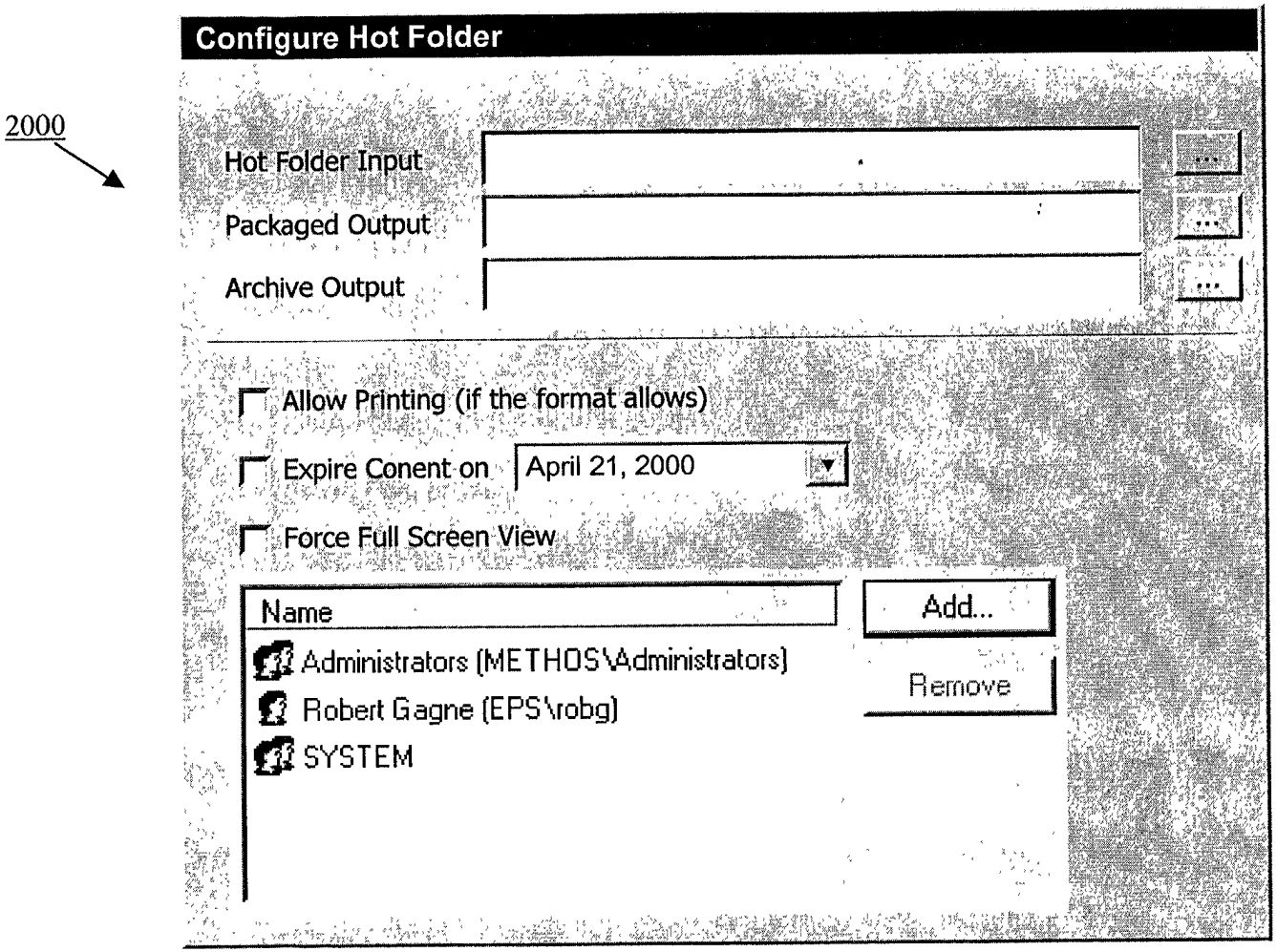

2000
Configure Hot Folder
Hot Folder Input
Packaged Output
Archive Output
...
...
...
Allow Printing (if the format allows)
Expire Conent on
April 21, 2000
Force Full Screen View
Name
Add...
Administrators (METHOS\Administrators)
Remove
Robert Gagne (EPS\robg)
SYSTEM

FIGURE 20

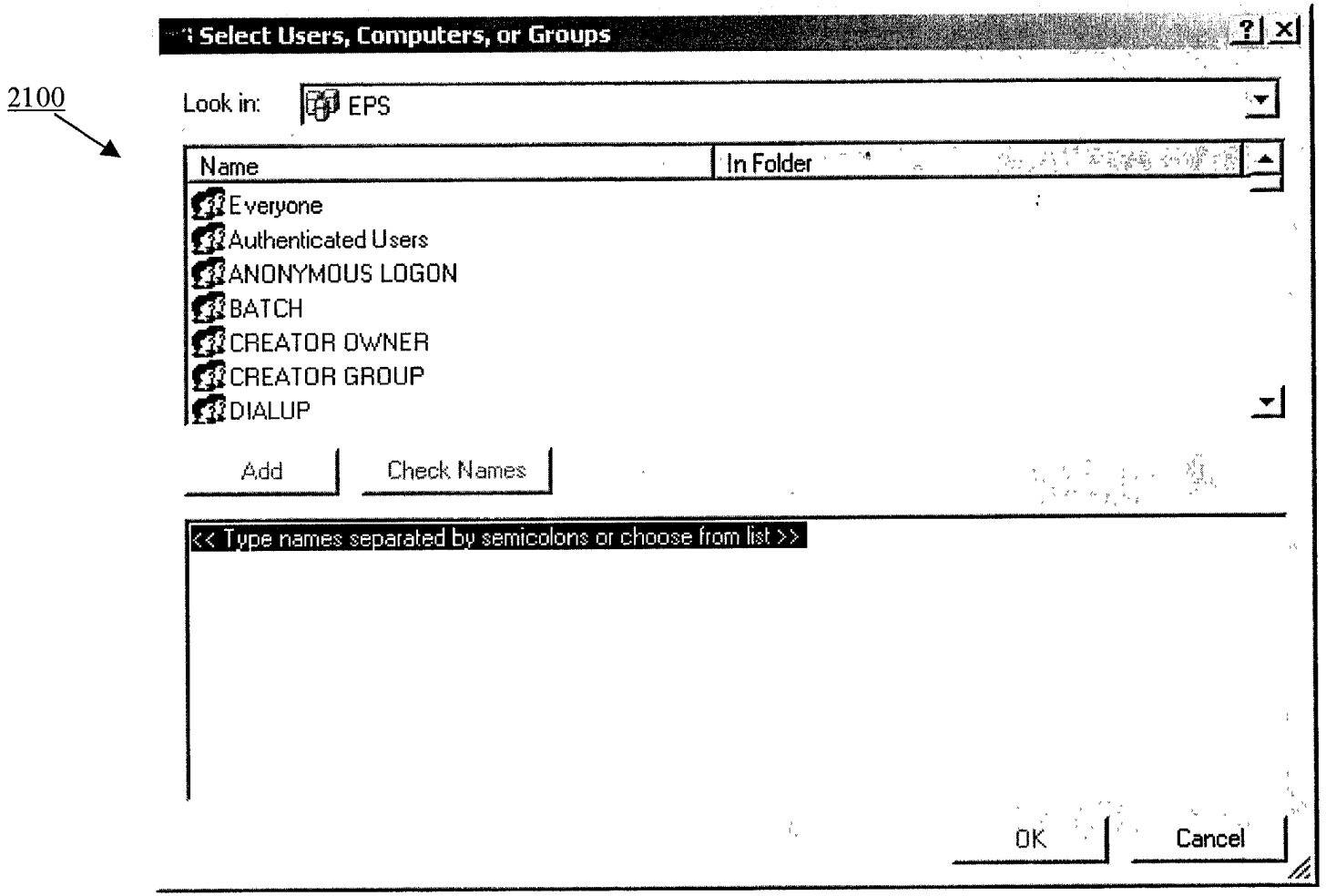

2100
Select Users, Computers, or Groups
Look in:
EPS
Name
In Folder
Everyone
Authenticated Users
ANONYMOUS LOGON
BATCH
CREATOR OWNER
CREATOR GROUP
DIALUP
Add
Check Names
<< Type names separated by semicolons or choose from list >>
OK
Cancel

FIGURE 21

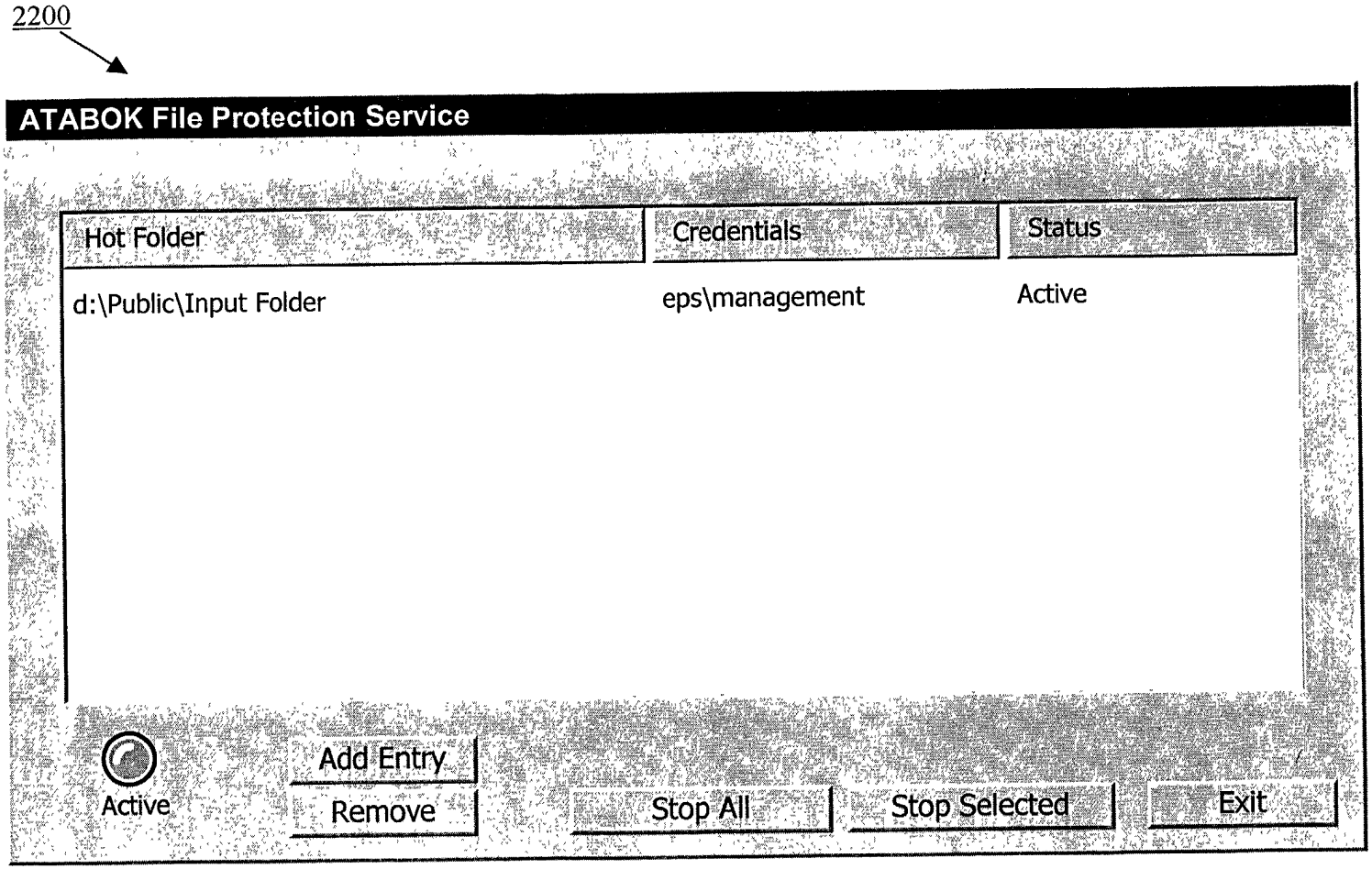

2200
ATABOK File Protection Service
Hot Folder
Credentials
Status
d:\Public\Input Folder
eps\management
Active
Active
Add Entry
Remove
Stop All
Stop Selected
Exit

FIGURE 22